

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
Middle District of PennsylvaniaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address.)Information associated with Instagram Account
Mrandrewhiggins, that is stored at premises controlled by
Meta Platforms, Inc.

Case No. 3:25-MC- 399

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18 U.S.C. Section 2422(b)	Attempted Online Enticement of a Minor

The application is based on these facts:

I, Kathryn Murray, a Special Agent with the Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SA Kathryn Murray

Applicant's signature

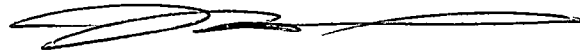
Kathryn Murray; SA-HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone _____ (specify reliable electronic means).

Date:

4/15/25



Judge's signature

City and state: Scranton, Pennsylvania

Phillip J. Caraballo, U.S. Magistrate Judge

Printed name and title

CONTINUATION SHEETS

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with the Instagram account **Mrandrewhiggins** identified in Attachment A (hereinafter referred to as the "SUBJECT ACCOUNT"), stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), a social networking provider headquartered at 1 Meta Way, Menlo Park, California 94025. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Instagram/Meta to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the SUBJECT ACCOUNT, including the contents of communications, as further described in Attachment B.

2. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), and have been employed in this capacity since August 2004. I am a graduate of the Criminal Investigator Training Program and ICE Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21, and 31 of the United States Code. I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

3. As part of my duties as an HSI agent, I investigate criminal violations relating to the sexual exploitation of children, including the illegal coercion and enticement of minors, and the production, distribution, receipt, and possession of child pornography, in violation of 18

U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the area of child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have participated in online undercover investigations which utilized messaging and social media platforms to interact with individuals interested in the enticement of a minor and the production, distribution, and/or receipt of child pornography. In my undercover role, I have become familiar with numerous social media platforms and the way in which digital devices are used to exploit children online as well as to transfer obscene images.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known concerning this investigation. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. As outlined in more detail below, I know that Title 18, United States Code, Section 2422(b) prohibits a person from using a facility of interstate commerce to knowingly persuade, induce, entice, and/or coerce a minor to engage in illegal sexual activity or attempting to do so

6. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. 2422(b) have been committed by Andrew HIGGINS who is believed to have utilized the SUBJECT ACCOUNT. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

8. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

STATUTORY AUTHORITY

9. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years to engage in prostitution, or any sexual activity for which any person can be charged with a criminal offense, or any attempts to do so.

DEFINITIONS

10. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output

devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

i. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from

its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. “Mobile application” or “chat application,” as used herein, are specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, digital, or magnetic form.

n. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation;

(d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), *aff'd sub nom, United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *aff'd*, 813 F.2d 1231 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987)

o. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

p. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

SUMMARY OF INVESTIGATION

11. Beginning on or about January 14, 2025, agents with Homeland Security Investigations conducted a proactive undercover operation aimed at locating and identifying individuals who utilize the internet and electronic devices to sexually exploit children.

12. Acting in an undercover capacity, 1, Special Agent Kathryn Murray, posed as “Cooper,” a 14-year-old male child.

13. On January 15, 2025, “Cooper” was messaged by a Grindr user without a username and then the communication shifted to text messaging. The communication, which was sexually

explicit in nature, was with an unknown male who utilized telephone number “386-301-2947.” Eventually, the unknown male was identified as Andrew HIGGINS (DOB: 09/15/1988).

14. The initial communication on Grindr included HIGGINS complimenting “Cooper’s” physical appearance and relaying his attraction to “Cooper.” Further, HIGGINS commented that “Cooper” not being responsive on the dating application Grindr. Soon after “Cooper” responded on Grindr, “Cooper” asked HIGGINS to switch to text messaging. “Cooper” provided HIGGINS with his cellular telephone number and HIGGINS sent, “Hi there” and “I’m the guy from the app. You gave me your contact.” HIGGINS provided the first name of “Drew” and then “Andrew.” “Cooper” informed HIGGINS that he was “14” to which HIGGINS responded “Jesus Christ” and “14yo.” “Cooper” told HIGGINS, “You don’t have to talk to me,” to which HIGGINS responded “Nah,” “I still think you’re cute,” and “Just wish you were older.” HIGGINS asked “Cooper” if he was a virgin to which “Cooper” stated he was. HIGGINS told “Cooper” that “everyone on that app fucks.” HIGGINS then stated, “I’m sure there are plenty guys who would still dick you down regardless of your age” and then stated, “Myself included.” “Cooper” asked HIGGINS what that meant, to which HIGGINS responded, “I would fuck you.” The conversation continued to discuss various sex acts that the two could do together, including “jerking off,” “oral,” “just foreplay,” “kissing,” and “fingering.”

15. Communication continued and “Cooper” told HIGGINS that he was going to his father’s apartment and would be skipping school on Friday. HIGGINS asked “Cooper” to participate in a video call. On January 15, 2025, SA Murray initiated a video call at approximately

2129hrs.¹ SA Murray observed an adult African American male with an accent on the video call and obtained a screenshot of the adult African American male.

16. HIGGINS stated: “I don’t wanna be catfished for trying to dick down a 14yo white boy.” HIGGINS asked “Cooper” for details about his first kiss with his male friend and with the adult he met on Grindr. HIGGINS asked if “Cooper” was a “top,” “bottom,” or “vers,” which I know from my training and experience are references to different sexual positions a male has with another male.

17. On January 16, 2024, HIGGINS stated, “You’re a 14yo boy,” “I’m an adult,” and “I don’t know the laws, but I feel like if someone were to set me up in a fake situation then I’d have a very hard time explaining myself enough to get out of problems.” “Cooper” and HIGGINS then discuss meeting in person on Friday, January 17, 2025. They planned to meet at a McDonald’s at 1171 North Ninth Street, Stroudsburg, Pennsylvania after HIGGINS’ completed an eye doctor appointment.

18. On January 16, 2025, Facial Recognition Technology (“FRT”) was used to search the probe photo (the screenshot SA Murray captured during the FaceTime video call) against a single repository of indexed, publicly available/open-source imagery. The FRT returned numerous publicly available images as potential matches. A review of the potential matches led SA Murray to the Instagram profile of Andrew HIGGINS with the username “Mrandrewhiggins” displayed and a profile for Andrew HIGGINS on the National Anti-Discrimination Alliance (“NADA”) website. SA Murray determined that all individuals in the pictures were the same individual.

¹ SA Murray was in a dark room with a hooded sweatshirt to conceal her face. SA Murray informed HIGGINS that “Cooper” could not speak because his mom would hear.

19. On January 17, 2025, HIGGINS stated that his eye doctor appointment was at 10:45 a.m. at America's Best in East Stroudsburg. Law enforcement set up surveillance and observed a male matching HIGGINS physical characteristics exit America's Best at 1159hrs and enter a white Infinity bearing Pennsylvania registration KPT-4382. At approximately 1212hrs, SA Murray observed that vehicle enter the parking lot of the McDonalds, the predetermined meet location. "Cooper" then received a text from HIGGINS stating, "Where are you?" "Cooper" responded that he was inside the McDonald's. Law enforcement observed HIGGINS exit the vehicle and walk towards the door to enter the McDonald's. HIGGINS was encountered by law enforcement prior to entering the restaurant. HIGGINS had two iPhones on his person when encountered by law enforcement at the restaurant. At approximately 1218hrs, SA Murray placed a confirmation call to the phone number HIGGINS was utilizing to text and observed "Cooper (Google)" on the screen.

20. HIGGINS was arrested by Pennsylvania State Police Corporal/Task Force Officer Jonathan Bailey and charged with Unlawful Contact with a Minor, Criminal Use of a Communication Facility, Solicitation to Commit Involuntary Deviate Sexual Intercourse, and Solicitation to Commit Statutory Sexual Assault. HIGGINS was transported to Monroe County Prison by Corporal Bailey and SA Murray without incident.

21. On March 10, 2025, law enforcement obtained a federal search warrant for both of the iPhones on HIGGINS' person at the time of his arrest, which was signed by the Honorable Pamela A. Carlos. Forensic analysis resulted in the extraction of some evidentiary artifacts pertaining to Instagram however, a full extraction was not successfully obtained. A search warrant of the SUBJECT ACCOUNT could aid law enforcement in the identification of other potential minors HIGGINS was communicating with on Instagram.

BACKGROUND CONCERNING INSTAGRAM²

22. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

23. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

24. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

25. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same

² The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," <https://privacycenter.instagram.com/policy/>; "Information for Law Enforcement," <https://help.instagram.com/494561080557017>; and "Help Center," <https://help.instagram.com>.

usernames at the same time. Instagram users can create multiple accounts and, if “added” to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

26. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

27. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

28. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can similarly allow Meta to search

an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

29. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography (“Bio”), and a website address.

30. One of Instagram’s primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users (“tag”), or add a location. These appear as posts on the user’s profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta’s servers.

31. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can “mention” others by adding their username to a comment followed by “@”). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

32. An Instagram “story” is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain on Meta’s servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

33. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

34. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

35. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

36. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily

searchable and can be “followed” to generate related updates from Instagram. Meta retains records of a user’s search history and followed hashtags.

37. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

38. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user’s identity and activities, and it can also reveal potential sources of additional evidence.

39. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

40. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

41. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where,

and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, voice messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

43. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to attempt communication with the victim of this investigation.

46. Therefore, Meta's servers are likely to contain all the material described above with respect to the Target Accounts, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CHARACTERISTICS OF OFFENDERS WHO COMMIT SEXUAL OFFENSES

AGAINST MINORS

49. From my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who commit sexual offenses against children using the internet often do so against multiple victims simultaneously or in quick succession, one after another. I have personally been involved in investigations involving online sexual exploitation of children where a single perpetrator exploited multiple minor victims. Furthermore, I am aware of cases involving a single perpetrator using the internet and specifically social media applications such as Instagram to exploit or attempt to exploit hundreds of victims.

50. Based on my training, knowledge, and experience, as well as my conversations with other law enforcement officers with whom I have had discussions about child exploitation investigations, I understand that individual(s) who use an electronic device(s) and the Internet to coerce and entice minors, as well as an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email or online storage account is likely to possess such information on additional digital storage devices and/or Internet email or online storage accounts that the individual possesses or controls. Additionally, based on this training and experience, I understand that even when the target uses a portable device (such as a cell phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found on other devices possessed by that individual.

51. I further know that subjects who attempt to sexually exploit minors online often possess sexually explicit content of minors. This content can be pictures or videos they received directly from victims, from other online sources, or from others who also sexually exploit children and possess child sexual abuse material. These same subjects also often send sexually explicit content to minors and others. This content includes photos and/or videos of themselves and sometimes of minor victims of sexual exploitation. Those who possess child sexual abuse material often do so on cell phones, tablets, computers, and external-storage media like hard drives, USB flash drives, SD cards, and micro-SD cards. From my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I know those who possess child sexual abuse material and attempt to exploit children online sometimes possess sexually explicit material in printed form and/or possess written documents detailing usernames and passwords of their own online accounts, usernames of the accounts of victims and/or coconspirators, and diaries relating to their conduct.

52. Based on the investigation to date, HIGGINS is an individual who has attempted to entice a minor.

CONCLUSION

53. Based on the forgoing, I request that the Court issue the proposed search warrant for the SUBJECT ACCOUNT described in Attachment A to require Instagram/Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Government-authorized persons will then review that information to locate the items described in Section II of Attachment B.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Instagram account that is stored at premises controlled by Meta Platforms, Inc. (“Meta”), a company that accepts service of legal process at 1 Meta Way, Menlo Park, California 94025.

Instagram Username: Mrandrewhiggins

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- A. All business records and subscriber information, in any form kept, pertaining to the account, including:
 - 1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 - 2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
 - 3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 - 4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 - 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 - 6. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and
 8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;
- B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata;
- C. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:
1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
 2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
 3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
 4. All associated logs and metadata;
- D. All content, records, and other information relating to all other interactions between the account and other Instagram users, including but not limited to:
1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
 2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
 3. All contacts and related sync information; and
 4. All associated logs and metadata;

- E. All records of searches performed by the account; and
- F. All location information, including location history, login activity, information geotags, and related metadata.

Meta is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. Sections 2422(b), 2251, 2252, and 1470 including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- A. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, including those in opened or unopened messages. These include both originals and copies.
- B. The contents of electronic communications, including attachments and stored files, including received messages, sent messages, deleted messages, and draft messages.
- C. All communications and files with or about potential minors involving sexual topics or communications aimed to induce, coerce, entice, or persuade a minor to engage in sexually explicit conduct.
- D. All visual depictions of child erotica;
- E. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256.

- F. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- G. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- H. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).
- I. The identity of the person(s) who communicated with the account holder about matters relating to the attempted online enticement of a minor, including records that help reveal their whereabouts.